블록체인 기반 홈페이지 위·변조 검증 프레임워크에 관한 연구#

이행곤*, 최장원*, 길준민**, 정용환*,##
*한국과학기술정보연구원 슈퍼컴퓨팅본부
**대구가톨릭대학교 IT공학부
e-mail: hglee1@kisti.re.kr, jwchoi@kisti.re.kr, jmgil@cu.ac.kr, paul7931@kisti.re.kr

A Study on the Framework of Block Chain-Based Website Falsification Verification

Heang-Gon Lee*, Jang-Won Choi*, Joon-Min Gil**, Yong-Hwan Jung*
*Korea Institute of Science and Technology Information
**School of Information Technology Engineering, Catholic Univ. of Daegu

요 약

최근 랜섬웨어 같은 치명적 신·변종 사이버공격에 의한 경제적 피해가 심각해지고 있는 실정이며, 취약 홈페이지에 대한 위·변조 공격은 사용자 PC의 악성코드 감염 경로로 활용되고 있다. 본 연구에서는 소스코드, 이미지 및 키워드 등 3가지 방식의 홈페이지 위·변조 검증을 수행하고 해당 결과를 블록체인 기반으로 관리하여 데이터의 투명성·보안성·안정성을 확보할 수 있는 프레임워크를 제시하고자 한다.

1. 서론

최근 페트야(Petya), 워너크라이(WanaCry) 랜섬웨어 같은 치명적인 신·변종 사이버공격이 첨예화·지능화됨에 따라 경제적인 피해 또한 급수적으로 증가하고 있는 추세이다. 특히 해킹조직이 경제적·정치적 목적 등을 달성하기 위해 취약한 홈페이지를 공격하여 해당 홈페이지를 위·변조시키는 공격은 악성코드 삽입이 주목적이며, 이러한 위·변조 공격은 일반 사용자 PC를 악성코드에 감염시키는 경로로 활용되며, 2차·3차 추가 피해를 발생시키는 진입 역할을 한다.

한편 블록체인 기술은 인공지능 및 빅데이터와 더불어 제4차 산업혁명을 견인할 핵심기술로 인식되고 있다. 블록체인 기술은 데이터를 중앙 집중화 시키지 않고 네트워크상의 여러 참여자 시스템들에 블록화하여 저장하여 분산원장 기술이라고도 불리며, 각 블록들은 서로 유기적으로 체인처럼 연결되어 있다. 블록체인 기술에 의한 분산 저장된 블록들의 유기적인 연결은 데이터의 투명성·보안성·안정성 제공이 특징이다. 이러한 특성들 때문에 블록체인 기술이 적용된 서비스 모델은 금융·핀테크 분야가 주를 이루고 있을 뿐, 다양한 ICT 분야에서 적용 연구만 이루어지고 있으며 실제 서비스가 이루어지는 모델은 전무하다.

본 연구는 ICT 분야 중 정보보호 분야에 블록체인 기술을 적용한 서비스 모델 발굴을 위해 홈페이지 위·변조 검증 서비스를 타겟 모델로 선정하였다. 기존의 어플라이언스 제품 위주의 홈페이지 위·변조 검증 제품은 제한된 하드웨어 사양에 의해 확장성이 부족하고, 외부의 공격에 의해 데이터가 유실·조작될 가능성이 존재한다. 이러한 한계를 극복하기 위해 본 연구에서 모든 참여자들이 위·변조 검증을 수행여하고, 검증된 결과를 블록체인으로 유지 및 관리하는 블록체인 기반의 홈페이지 위·변조 검증 프레임워크를 제안하여 데이터의 투명성·보안성·안정성 및 인프라의 확장성을 확보하고자 한다.

본 연구는 (2017년도) 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다
교신저자(paul7931@kisti.re.kr)

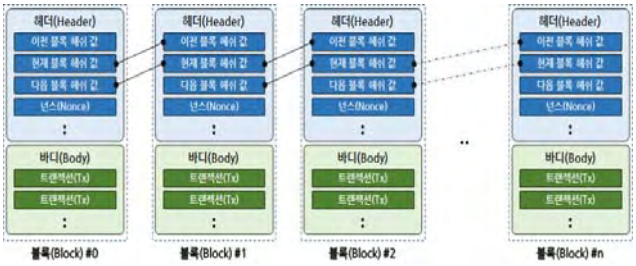
2. 관련 연구

2.1 블록체인 기술의 정의

블록체인은 세계 최초의 가상 암호 화폐인 비트코인에서 처음 나타난 개념으로 거래정보가 중앙 서버에 집중되지 않고 네트워크의 여러 컴퓨터에 분산해서 저장하는 것'을 말하며, 특정한 여러 정보들을 담은 컴퓨터 코드들로 이뤄진 블록(block)들이 서로 유기적으로 묶여 사슬(chain)처럼 이어져있어 블록체인이라 한다.

여기서 블록(Block)이라함은 여러 정보를 담고 있는 폴더로 특정한 시간 동안 거래된 거래내역과 관련 정보를 묶어서 하나의 파일을 만드는 것으로 비트코인의 경우 10분마다 하나의 블록이 생성된다. 하나의 블록은 헤더(Header)와 바디(Body)로 이루어져 있으며, 헤더에는 현재 블록을 이전 블록과 다음 블록을 연결하는 해쉬(Hash) 값과 암호화된 시스템에서 사용되는 임의의 수인 넌스(Nonce) 등이 포함되어 있으며, 바디에는 거래별 트랜잭션(Transaction)이 기록되어 있다. 블록들은 각각의 파일로 분리되어 있지만, 특정시간 마다 새롭게 생성되는데 신

규 블록이 형성될 때 기존의 블록에 계속 연결되는 구조를 체인(Chain)이라 하며 (그림 1)은 블록체인의 연결 구조를 보여준다.



(그림 1) 블록체인의 연결구조[2]

2.2 블록체인 기술의 장점

블록체인 기반 환경에서는 데이터가 네트워크 상의 분산노드들에 복제되어 저장되기 때문에 <표 1>과 같이 보안성, 안전성, 투명성과 같은 장점을 가진다.

<표 1> 블록체인 기술의 장점[3]

구분		설명
장점	보안성	-모든 정보가 집중된 중앙 서버가 없고 이를 담당하는 조직도 존재하지 않기 때문에 해킹 등 내·외부의 악의적인 공격으로부터 안전 -원장이 모든 참가자에게 공개되기 때문에 원천적으로 정보유출 소지가 없음
	안전성	-모든 참여자가 동일한 정보가 담긴 파일을 분산·저장·관리 -일부 네트워크 장애는 전체 블록체인에 영향을 미치지 않음
	투명성	-모든 거래기록이 공개되어 투명성이 높아, 거래 추적이 용이하며 규제준수 비용도 낮음
	불변성	-블록체인을 변경하기는 거의 불가능하기 때문에 정보의 신뢰성 증가 -거래의 취소가 불가능하여 기록의 정확성을 증가시키며, 백오피스 과정을 간소화 시킴

2.3 블록체인의 종류

블록체인 은 네트워크 참가자의 성격 및 범위에 따라 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain), 컨소시엄 블록체인 혹은 하이브리드(Consortium or Hybrid Blockchain)으로 구분되며, 블록체인의 유형별 특징은 <표 2>와 같다.

<표 2> 블록체인 유형별 특징 및 예시[3]

구분	퍼블릭 블록체인	프라이빗 블록체인	컨소시엄 블록체인
개념 및 특징	-최초의 블록체인 활용 사례 -인터넷을 통해 모두에게 공개, 운용 가능한 거래장부 -컴퓨터 파워를 네트워크에 제공함으로써 누구든 공증에 참여 -네트워크 확장이 어렵고 거래 속도가 느림	-개인형 블록체인 -1개의 주체가 내부 전산망을 블록체인으로 관리 -프라이빗 블록체인 개발을 위한 플랫폼 서비스 등장	-반 중앙형 블록체인 -미리 선정된 N개의 주체들만 참여 가능 -N개의 주체들 간의 합의된 Rule 등을 통해 공증 참여 -네트워크 확장이 용이하고 거래 속도가 빠름
주요 니즈/ 선결 요건	-네트워크 효과 -안정적 생태계 -위험관리	-시스템 변경 감수/ 안정성 확보 -1개의 주체 내 글로벌 브런치	-참여주체들 간의 비즈니스적인 동의/합의 -시스템 안정성 확보
예시	Bitcoin, Ripple, Litecoin, Ethereum 등	NASDAQ, Overstock, Chain 등	R3CEV, HSBC, Citi, Barclays, Goldman Sachs, BoA 등

3. 블록체인 기반 홈페이지 위·변조 검증 프레임워크

3.1 프라이빗 블록체인 구성 및 노드 유형별 역할

본 연구에서는 블록체인 기반 홈페이지 위·변조 검증을 위해 중앙노드에 의해 제어될 수 있는 프라이빗 블록체인 유형을 선택하였다. 이는 미리 지정된 홈페이지에 대해서만 정의된 규칙에 따라 위·변조 탐지를 제한된 참여자들의 분산노드만 수행한다.

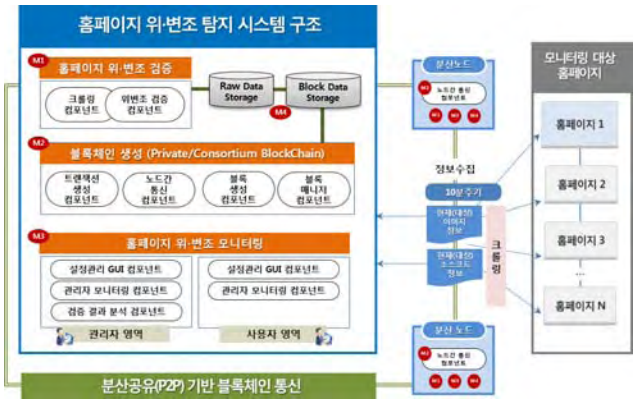
이러한 홈페이지 지정, 규칙의 정의, 참여자 제한은 중앙노드에서 통제·제어한다. 볼륵체인 기반 홈페이지 위·변조 검증에 참여하는 중앙노드 및 모든 참여노드들은 P2P 네트워크 통신을 통해 데이터(블록)을 생성·공유하며, <표 3>은 모든 참여 노드들의 유형별 수행 역할을 설명한다.

<표 3> 참여 노드 유형별 수행 역할

노드 유형	수행 역할	
	공통 수행 역할	노드별 특화 역할
중앙 Main 노드	-10분 주기로 대상 사이트 현재 상태 수집 및 위·변조 검증 -위·변조 검증 결과 전송 -일정 시간동안 수집된 검증 결과의 블록화 및 전송	-24시간 주기로 모든 노드에서 검증할 원본 데이터 수집 -모든 참여 노드에 원본데이터 및 정책데이터(블록) 전송 -모든 참여 노드에 머신러닝 학습 및 학습 결과 전송 -모든 노드에서 검증 결과를 취합하여 모니터링 시스템에 출력
중앙 Slave 노드		-중앙노드 Main Fail 시 Main 역할 수행
분산 노드		-분산노드 관리자 지정 페이지를 24시간 주기로 수집 및 머신러닝 학습(원본 데이터) -분산노드 관리자 지정 페이지를 10분 주기로 대상 사이트 현재 상태 수집 및 검증 -원본 데이터와 수집된 데이터를 비교하여 위·변조 탐지

3.2 프레임워크 설계

블록체인 기반 홈페이지 위·변조 탐지를 위한 시스템은 폼페이지 정보를 수집 및 비교하여 위·변조 여부를 검증하는 “홈페이지 위·변조 검증 모듈(M1)”, 위·변조 검증에 활용된 정보들을 블록으로 만들어 저장하는 “블록체인 생성 모듈(M2)”, 위·변조 결과를 관리자가 모니터링하는 “홈페이지 위·변조 모니터링 모듈(M3)” 3개와 해당 시스템에서 발생되는 모든 정보들을 저장하는 “Raw_Data Storage 및 Block_Data Storage”로 이루어져 있다.



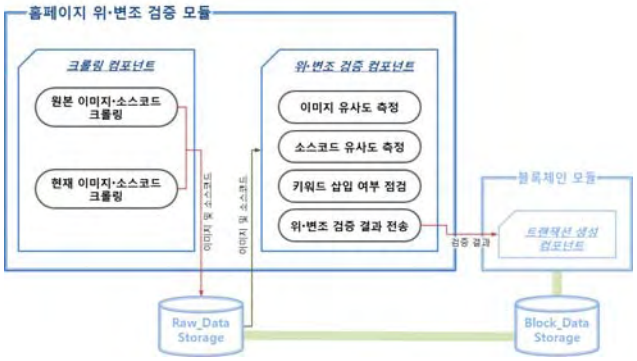
(그림 2) 블록체인 기반 위·변조 탐지 시스템 구조

3.2.1 홈페이지 위·변조 검증 모듈

홈페이지 위·변조 검증 모듈은 24시간 주기마다 원본 데이터(메인페이지 스냅샷, 소스코드)를 크롤링하여 저장한 뒤, 이를 관리자 설정 주기마다 수집되는 데이터와 비교하여 위·변조 여부를 점검하는 모듈로 「크롤링 컴포넌트」「위·변조 검증 컴포넌트」로 구성된다.

크롤링 컴포넌트는 사용자가 설정한 URL들의 메인화면 스냅샷과 소스코드 수집, 매일 0시에 원본으로 삼을 홈페이지 정보 수집, 사용자 설정 주기마다 대상 URL들을 방문하여 비교할 스냅샷과 소스코드 수집 하는 역할을 수행한다.

위·변조 검증 컴포넌트는 이미지, 소스코드, 키워드 방식 등 3가지 방식에 의한 위·변조 여부를 검증하고, 검증결과들을 블록체인 모듈의 트랜잭션 생성 컴포넌트로 전달하여 각 참여노드에 전송할 수 있도록 한다.



(그림 3) 홈페이지 위·변조 검증 모듈 개념도

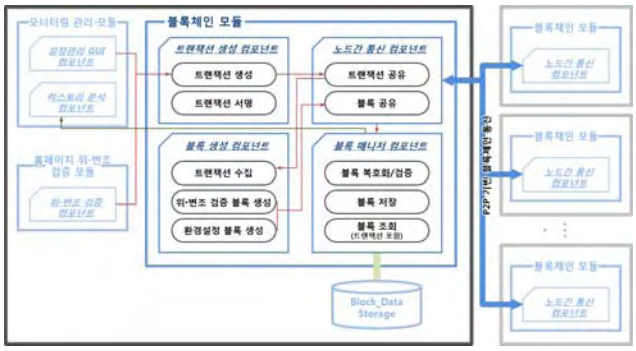
3.2.2 블록체인 모듈

블록체인 모듈은 P2P 네트워크 통신으로 모든 참여노드에서 생성된 트랜잭션을 공유하고 공유된 트랜잭션들을 수집하여 블록 생성·검증·조회 역할을 수행하는 모듈로 「트랜잭션 생성 컴포넌트」「블록 생성 컴포넌트」「노드 간 통신 컴포넌트」「블록 매니저 컴포넌트」로 구성된다.

트랜잭션 생성 컴포넌트는 위·변조 검증 결과 및 각 노드에 적용될 환경설정 등을 트랜잭션으로 생성하고, 생성된 트랜잭션을 공유하기 위해 「노드 간 통신 컴포넌트」로 전달한다. 노드는 자신이 생성한 트랜잭션임을 증명하기 위하여 노드 자신의 고유한 비밀키로 트랜잭션에 서명하는 역할을 수행한다.

블록 생성 컴포넌트는 각 참여 노드로부터 공유된 트랜잭션들을 수집하여 블록을 생성하고, 생성된 블록을 참여 노드에 전송하기 위해 「노드 간 통신 컴포넌트」로 전달하는 역할을 수행한다. 여기서 블록은 위·변조 검증에 사용된 데이터(위·변조 검증 데이터 블록)와 환경 설정 정보(환경 설정 블록) 등 두 가지의 정보를 포함하고, 위·변조 검증 데이터 블록은 사전 정의된 알고리즘에 따라 전체 노드 중 하나의 노드에서만 생성되고, 환경 설정 블록은 중앙 Main 노드(관리 노드)에서만 생성하여 전체 참여 노드에 공유한다.

노드 간 통신 컴포넌트 모든 노드 간 P2P통신을 통해 트랜잭션 및 블록 공유하는 역할을 수행하며, 블록 매니저 컴포넌트는 공유된 블록의 검증/저장 기능제공 및 사용자 권한에 따라 허용된 트랜잭션 정보 조회 기능을 수행한다.



(그림 4) 블록체인 모듈 개념도

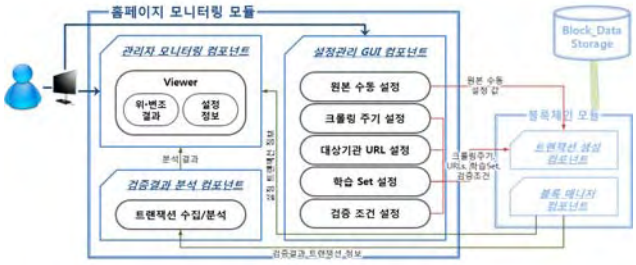
3.2.3 홈페이지 모니터링 모듈

홈페이지 모니터링 모듈은 관리자가 위·변조 현황 모니터링 및 프라이빗 블록체인 구성·관리 기능을 제공하는 모듈로 「관리자 모니터링 컴포넌트」「설정관리 GUI 컴포넌트」「검증결과 분석 컴포넌트」로 구성된다.

관리자 모니터링 컴포넌트는 관리자 설정 URL들의 위·변조 검증 결과 및 설정 값에 대한 모니터링 기능 제공하고, 과거 24시간 동안의 위·변조 모니터링 결과를 한눈에 볼 수 있으며, 원본과 대상이미지 현황을 비교하여 변조로 의심되는 부분을 시각적으로 표시하여 관리자에게 직관성 부여하는 역할을 수행한다.

설정관리 GUI 컴포넌트는 프라이빗 블록체인 구성 및 위·변조 검증에 필요한 다양한 설정 기능을 GUI를 통해 제공하는 역할을 수행한다.

검증결과 분석 컴포넌트는 위·변조 검증 결과 블록에 포함된 정보들을 분석하여 낮은 매칭결과를 보이는 URL의 정보를 관리자 모니터링 컴포넌트에 전달하는 역할을 수행한다.



(그림 5) 홈페이지 모니터링 모듈 개념도

4. 결론 및 향후 계획

본 논문에서는 프라이빗 블록체인 기반의 홈페이지 위·변조 검증 시스템의 프레임워크를 제시하여, 내부 구조와 각 모듈별 기능과 프레임워크를 살펴보았다. 향후에는 설계된 프레임워크를 기반으로 200여개 홈페이지에 대한 홈페이지 위·변조를 검증할 수 있도록 오픈소스 기반으로 개발하고 시스템을 구축하여 실제 환경에 적용할 예정이다.

참고문헌

[1] “2016 하이프사이클 - 블록체인/프로그래머블 경제”, 가트너 그룹, 2016. 7.

[2] “국내외 금융분야 블록체인 활용동향”, 금융보안원, 2015

[3] 고윤승·최홍섭, “비즈니스 패러다임 변화와 그 활용방안”, 한국과학예술포럼, 2017. 1.

[4] “블록체인 개발 플랫폼 현황 및 활용 사례”, 금융보안원, 2016.10.

[5] “블록체인기술 개념 및 적용현황”, 한국전자통신연구원

[6] “블록체인 및 관련 보안표준화 추진동향”, 한국정보통신기술협회

[7] 블록체인이 가져오는 우리의 미래모습, IBM, 2017

[8] Pete Rizzo, “Blockchain Land Title Project ‘Stalls’ in Honduras”, Coindesk, 2015.12.26